



Jordi Pujolàs Boix

Dades personals-contacte / Datos personales-contacto / Personal information-contact



Jordi Pujolàs Boix

Professora:

Professor Agregat interí / Profesor Agregado interino / Associate p

Matemàtica Aplicada / Matemática Aplicada / Applied Mathematics

/Department:

Matemàtica / Matemática / Mathematics

Centre/Centro/Center:

Escola Politècnica Superior / Escuela Politècnica Superior/ Polyte

Despatx/Despacho/Office:

Campus de Cappont. Edifici EPS. Despatx 1.20 / Campus de
Despacho 1.20 / Campus of Cappont. EPS Building. Office 1.20



jpujolas@matematica.udl.cat

mailto:jpujolas@matematica.udl.



+34 973 70 27 43

Code ORCID:

<https://orcid.org/0000-0002-1192-8192>

<https://orcid.org/0000-0002-1192-8192>



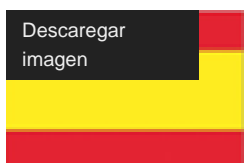
TORNAR AL LLISTAT / VOLVER AL LISTADO / BACK TO LIST [
/sites/Eps/ca/lescola/organitzacio/personal-docent-i-investigador/]

Formació acadèmica / Formación académica / Academic training



--2006

- Llicenciat en Matemàtiques, Universitat Autònoma de Barcelona --1998
- Professor de Piano (grau mitjà), Conservatori Superior Municipal de Música de Barcelona (Bruc) --1997
- Doctor per la Universitat Politècnica de Catalunya, programa de doctorat en Matemàtiques



- Licenciado en Matemáticas, Universitat Autònoma de Barcelona – 1998
- Profesor de Piano (grado medio), Conservatorio Superior Municipal de Música de Barcelona (Bruc) --1997
- Doctor por la Universitat Politècnica de Catalunya, programa de doctorado en Matemáticas --2006
- Degree in Mathematics, Universitat Autònoma de Barcelona --1998
- Piano Degree , Conservatori Superior Municipal de Música de Barcelona (Bruc) – 1997



Descargar imagen

- PhD Universitat Politècnica de Catalunya (Mathematics) – 2006



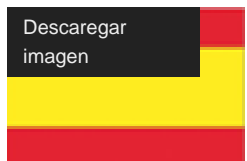
TORNAR AL LLISTAT / VOLVER AL LISTADO / BACK TO LIST [/sites/Eps/ca/lescola/organitzacio/personal-docent-i-investigador/]

Experiència professional / Experiencia profesional / Professional experience



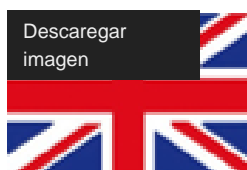
Descargar imagen

- Pofessor Associat -- Universitat Autònoma de Barcelona 1999 – 2004
- Becari Predoctoral -- Universitat Politècnica de Catalunya-Royal Holloway University of London 2004 - 2006
- Professor Visitant -- Universitat de Lleida 2006 - 2009
- Becari Postdoctoral -- Acadèmia Xinesa de les Ciències, Universitat de Zuric, Universitat de Lleida 2009 - 2012
- Professor Lector -- Universitat de Lleida 2013 - 2017
- Professor Agregat Interí -- Universitat de Lleida 2017 - 2019



Descargar imagen

- Profesor Asociado -- Universitat Autònoma de Barcelona 1999 - 2004
- Becario Predoctoral -- Universitat Politècnica de Catalunya-Royal Holloway University of London 2004 - 2006
- Profesor Visitante -- Universitat de Lleida 2006 - 2009
- Becario Postdoctoral -- Academia China de las Ciencias, Universidad de Zurich, Universitat de Lleida 2009 - 2012
- Profesor Lector -- Universitat de Lleida 2013 - 2017
- Profesor Agregado interino -- Universitat de Lleida 2017 - 2019



Descargar imagen

- Assistant -- Universitat Autònoma de Barcelona 1999 - 2004
- Predoc -- Universitat Politècnica de Catalunya-Royal Holloway University of London 2004 - 2006
- Visiting Professor -- Universitat de Lleida 2006 - 2009
- Postdoc -- Chinese Academy of Science, University of Zurich, Universitat de Lleida 2009 - 2012
- Lecturer -- Universitat de Lleida 2013 - 2017
- Associate Professor -- Universitat de Lleida 2017 - 2019



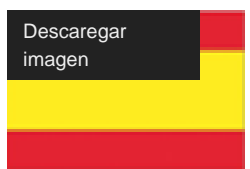
TORNAR AL LLISTAT / VOLVER AL LISTADO / BACK TO LIST [/sites/Eps/ca/lescola/organitzacio/personal-docent-i-investigador/]

Docència / Docencia / Teaching

- Grau en Enginyeria Informàtica



- Grau en Enginyeria Mecànica
- Grau en Enginyeria Electrònica Industrial i Automàtica
- Grau en Enginyeria de l'Energia i Sostenibilitat
- Doble Grau en Enginyeria Informàtica i Administració i Direcció d'Empreses



- Grado en Ingeniería Informática
- Grado en Ingeniería Electrónica Industrial y Automática
- Grado en Ingeniería Mecánica
- Grado en Ingeniería de la Energía y Sostenibilidad
- Doble Grado en Ingeniería Informática y Administración y Dirección de Empresas



- Degree in Computer Engineering
- Degree in Industrial Electronics and Automatic Engineering
- Degree in Mechanical Engineering
- Degree in Energy Engineering and Sustainability
- Double Degree in Computer Engineering and Business Administration and Management

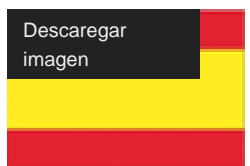


TORNAR AL LLISTAT / VOLVER AL LISTADO / BACK TO LIST [</sites/Eps/ca/lescola/organitzacio/personal-docent-i-investigador/>]

Gestió / Gestión / Management



- Representant de Campus a la Comissió de Biblioteques de la UdL
- Responsable del Pla Nestor a la EPS.



- Representante de Campus en la Comisión de Bibliotecas de la UdL
- Responsable del Plan Nestor en la EPS



- Campus representative in the UdL Libraries Commission
- Responsible for the Nestor Plan in EPS

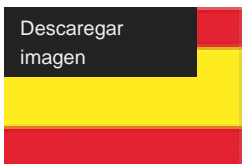


TORNAR AL LLISTAT / VOLVER AL LISTADO / BACK TO LIST [</sites/Eps/ca/lescola/organitzacio/personal-docent-i-investigador/>]

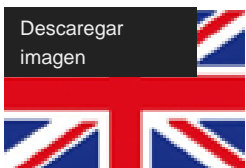
Recerca / Investigación / Research

Àmbit de recerca / Ambito de investigación / Research area

- Teoria de Nombres computacional i criptografia.



Teoría de Números Computacional y Criptografía



Computational Number Theory and Cryptography

Activitats de recerca / Actividades de investigación / Research activities



Acreditació de Recerca AQU –23/04/2018

2 Trams de Recerca AQU (2010, 2017)

Tesis Doctorals Dirigides 1

Publicacions: 15 (WoS), Total Cites 43 (WoS), h-index 4 (WoS)

Projectes Europeus:

“Solucions de seguretat i ciber-seguretat en utilitats per a protecció d'infraestructures crítiques”, Comunitat Ris3cat: Utilities 4.0 (Acció: Fons Europeu FEDER), COMRDI16-1-0060, 2017 - 2020, IPs: Josep M. Miret Biosca, Francisco Sebé Feixas

Altres Projectes de recerca:

“Criptografía y códigos para aplicaciones seguras y fiables”, Ministerio de Ciencia, Innovación y Universidades, MTM2017-83271-R, 2018 - 2020, IPs: Francisco Sebé Feixas, Magda Valls Marsal

“Criptografía con Curvas Algebraicas para la e-Sociedad”, Ministerio de Economía y Competitividad, MTM2013-46949-P, 2014 - 2017, IPs: Josep M. Miret Biosca; Francisco Sebé Feixas

“Number Theoretic Algorithms inspired by Cryptography”, Comisión Nacional de Investigación Científica y Tecnológica (CONICYT), Gobierno de Chile, FONDECYT 1110578, 2011 - 2015, IP: Nicolas Thériault

“BallotNext: Diseño y desarrollo de un sistema de votación avanzado basado en papel (INNPACTO)”, Ministerio de Economía y Competitividad, IPT-2012-0603-430000, 2013 - 2014, IP: Josep M. Miret Biosca

Publicacions:



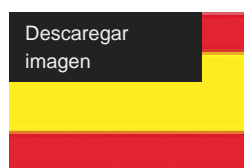
J. M. Miret, J. Pujolàs, N. Thériault, "Bisection and squares in genus 2", *Finite Fields and Their Applications*, 36, 170-188 (2015)

J.M. Miret, J. Pujolàs, N. Thériault, "Trisection for supersingular genus 2 curves in characteristic 2", *Advances In Mathematics of Communications*, 8 (4), 375-387 (2014)

J.M. Miret, J. Pujolàs, A. Rio, "Bisection for genus 2 curves in odd characteristic", *Proceedings of the Japan Academy Series A - Mathematical Sciences*, 85 (4), 55-61 (2009)

S. Galbraith, J. Pujolàs, Ch. Ritzenthaler, B. Smith, "Distortion maps for supersingular genus two curves", *Journal of Mathematical Cryptology*, 3 (1), 1-18 (2009)

G. Cardona, E. Nart, J. Pujolàs, "Curves of genus two over fields of even characteristic", *Mathematische Zeitschrift*, 250 (1), 177-201 (2005)



Acreditación de investigación AQU –23/04/2018

2 Sexenios de investigación AQU (2010, 2017)

Tesis Doctorales Dirigidas 1

Publicaciones: 15 (WoS), Total Citas 43 (WoS), índice h 4 (WoS)

Proyectos Europeos:

"Solucions de seguretat i ciber-seguretat en utilitats per a protecció d'infraestructures crítiques", Comunitat Ris3cat: Utilitats 4.0 (Fondo Europeo FEDER), COMRDI16-1-0060, 2017 - 2020, IPs: Josep M. Miret Biosca, Francisco Sebé Feixas

Otros Proyectos de investigación:

"Criptografía y códigos para aplicaciones seguras y fiables", Ministerio de Ciencia, Innovación y Universidades, MTM2017-83271-R, 2018 - 2020, IPs: Francisco Sebé Feixas, Magda Valls Marsal

"Criptografía con Curvas Algebraicas para la e-Sociedad",

Ministerio de Economía y Competitividad, MTM2013-46949-P, 2014 - 2017, IPs: Josep M. Miret Biosca; Francisco Sebé Feixas

"Number Theoretic Algorithms inspired by Cryptography", Comisión Nacional de Investigación Científica y Tecnológica (CONICYT), Gobierno de Chile, FONDECYT 1110578, 2011 - 2015, IP: Nicolas Thériault

"BallotNext: Diseño y desarrollo de un sistema de votación avanzado basado en papel (INNPACTO)", Ministerio de Economía y Competitividad, IPT-2012-0603-430000, 2013 - 2014, IP: Josep M. Miret Biosca

Publicaciones:

J. M. Miret, J. Pujolàs, N. Thériault, "Bisection and squares in genus 2", *Finite Fields and Their Applications*, 36, 170-188 (2015)

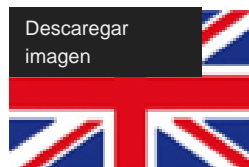
J.M. Miret, J. Pujolàs, N. Thériault, "Trisection for supersingular genus 2 curves in characteristic 2", *Advances In Mathematics of Communications*, 8 (4), 375-387 (2014)

J.M. Miret, J. Pujolàs, A. Rio, "Bisection for genus 2 curves in odd characteristic", *Proceedings of the Japan Academy Series A - Mathematical Sciences*, 85 (4), 55-61 (2009)



S. Galbraith, J. Pujolàs, Ch. Ritzenthaler, B. Smith, “Distortion maps for supersingular genus two curves”, *Journal of Mathematical Cryptology*, 3 (1), 1-18 (2009)

G. Cardona, E. Nart, J. Pujolàs, “Curves of genus two over fields of even characteristic”, *Mathematische Zeitschrift*, 250 (1), 177-201 (2005)



Researcher Credential AQU –23/04/2018

2 official six-year research periods AQU (2010, 2017)

Advised PhDs 1

JCR Papers: 15 (WoS), Total Citations 43 (WoS), h-index4 (WoS)

European Projects:

“Solucions de seguretat i ciber-seguretat en utilitats per a protecció d'infraestructures crítiques”, Comunitat Ris3cat: Utilities 4.0 (European Fund FEDER), COMRD16-1-0060, 2017 - 2020, PRs: Josep M. Miret Biosca, Francisco Sebé Feixas

Other research projects:

“Criptografía y códigos para aplicaciones seguras y fiables”, Ministerio de Ciencia, Innovación y Universidades, MTM2017-83271-R, 2018 - 2020, PRs: Francisco Sebé Feixas, Magda Valls Marsal

“Criptografía con Curvas Algebraicas para la e-Sociedad”,

Ministerio de Economía y Competitividad, MTM2013-46949-P, 2014 - 2017, PRs: Josep M. Miret Biosca; Francisco Sebé Feixas

“Number Theoretic Algorithms inspired by Cryptography”, Comisión Nacional de Investigación Científica y Tecnológica (CONICYT), Gobierno de Chile, FONDECYT 1110578, 2011 - 2015, PR: Nicolas Thériault

“BallotNext: Diseño y desarrollo de un sistema de votación avanzado basado en papel (INNFACTO)”, Ministerio de Economía y Competitividad, IPT-2012-0603-430000, 2013 - 2014, PR: Josep M. Miret Biosca

Journal Papers:

J. M. Miret, J. Pujolàs, N. Thériault, “Bisection and squares in genus 2”, *Finite Fields and Their Applications*, 36, 170-188 (2015)

J.M. Miret, J. Pujolàs, N. Thériault, “Trisection for supersingular genus 2 curves in characteristic 2”, *Advances In Mathematics of Communications*, 8 (4), 375-387 (2014)

J.M. Miret, J. Pujolàs, A. Rio, “Bisection for genus 2 curves in odd characteristic”, *Proceedings of the Japan Academy Series A - Mathematical Sciences*, 85 (4), 55-61 (2009)

S. Galbraith, J. Pujolàs, Ch. Ritzenthaler, B. Smith, “Distortion maps for supersingular genus two curves”, *Journal of Mathematical Cryptology*, 3 (1), 1-18 (2009)



G. Cardona, E. Nart, J. Pujolàs, "Curves of genus two over fields of even characteristic", *Mathematische Zeitschrift*, 250 (1), 177-201 (2005)



TORNAR AL LLISTAT / VOLVER AL LISTADO / BACK TO LIST [
/sites/Eps/ca/lescola/organitzacio/personal-docent-i-investigador/]